



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/029,686	12/21/2001	Herbert V. Joiner	NA11P065/01.307.01	3317
28875	7590	03/01/2005	EXAMINER	
Zilka-Kotab, PC P.O. BOX 721120 SAN JOSE, CA 95172-1120			SON, LINH L D	
			ART UNIT	PAPER NUMBER
			2135	

DATE MAILED: 03/01/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>		<b>Applicant(s)</b>	
	10/029,686		JOINER, HERBERT V.	
	<b>Examiner</b>		<b>Art Unit</b>	
	Linh Son		2135	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 12/21/2001.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-37 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-37 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date <u>10/04</u> . | 6) <input type="checkbox"/> Other: _____  |

### DETAILED ACTION

1. The written action is responding to the Amendment received on July 15 of 2005.

Claims 1-37 are pending. Claims 1,6,11,15,21,22,25, and 27 are amended. Claims 29-37 are newly added claims.

### ***Claim Rejections - 35 USC § 103***

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. **Claims 1, 3-6, 8-11, 13-16, 18-22, and 25-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Drake et al, US Patent No. 6347374A1, hereinafter "Drake", in view of Porras et al, US Patent No. 6704874B1, hereinafter "Porras".**

4. As per claim 1, 3, 6, 8, 11, 13, 16, 18, 21, 25, and 27, Drake discloses the "Event Detection" invention, which includes a method for analyzing a network, scanning the network, and detecting intrusions in the network. The system comprises: Collector (agent), Parsers, Generic File Transfer Utility (GFTU), Inserter, Database, Expert System Engines (ESG) (Host Controller), and Manager/configuration GUI (Zone Controller) (See Figure 1). The collector is an agent running on computers on the

network and there are different collectors associated to the applications monitoring (Col 9 lines 53-59). GFTU, locating on the client computer, sends data files, such as log files or other files depending on the application to the parser (Col 9 line 65 to Col 10 line 4).

The Parser is located on the remote network collecting the data files, parses, and then passes the data files in Virtual Record format readable by the ESG to the Inserter (Col 7 lines 38-54, and Col 10 lines 21-32). The Inserter stores the records in the database.

The ESG has many functions or controllers, such as deriving database information to detect events, Hard-Coded processor, Execution array based processors, and Rule-based interpreters (Col 11 lines 7-17, line 52 to Col 13 line 67). ESG utilizes the controllers above to analyze and detect intrusion (Col 7 line 51, and Col 11 line 53 Col 12 line 67), and creates events model and report for the network (Col 15 lines 59-62).

The Manager/Configuration GUI takes all the output data from ESG and generates reports or statistical data accordingly (Col 17 lines 1-24). The Manager/Configuration GUI also has admin capability to configure rule-based triggers to the event. However, Drake does not teach the Zone Controller specifically. Nevertheless, Drake teaches the ESG, which has the HC and ZC functionalities as claimed and part is in the Manager/Configuration GUI (See above citing). Therefore, it is obvious at the time of the invention for one of ordinary skill in the art to separate both components to minimize the processing time and load. Further, Drake teaches the generation of the report from the report including a plurality of objects; wherein intrusion detection services are provided based on the information (Col 17 lines 25-59); and a capability to transfer the alert data (Col 9 line 60 to Col 10 line 20). However, Drake does not teach the report in

Art Unit: 2135

a tree representation, and the simple network management protocol (SNMP) trap capability is utilized. Nevertheless, the report in a tree representation is the designer choice. In regard to the implementation of SNMP trap to receive alert is taught clearly in Porras. Porras discloses the "Network-Based Alert Management" invention, which includes a network manager (Zone Controller) receiving alerts from a plurality of devices in the network utilized SNMP and other transfer protocol (Col 3 line 15 to Col 4 line 67, and Col 7 line 18 to Col 8 line 67). Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Drake's invention to include the report with the tree representation and also the teaching of Porras to transfer the alert data in real time and respond quickly.

5. As per claims 4, 9, 14, and 19, Drake and Porras disclose the systems as recited in claim 1, wherein "the host controllers and the zone controllers operate based on business rules" is taught by Drake in (Col 17 lines 15-24).

6. As per claims 5, 10, 15, and 20, Drake and Porras disclose the system as recited in claim 1, wherein "the business rules are user-configurable" is taught by Drake in (Col 17 lines 15-24).

7. As per claim 22, claim 1 rejection basis is applied. Further, Drake discloses a method to configure and identifying the business rules applicable to the network users and services in (Col 5 lines 36-60 and Col 17 lines 1-24).

8. As per claims 26 and 28, Drake and Porras disclose the system as recited in claim 25, wherein “the information relates to wireless network traffic” is taught by Drake in (Col 5 lines 48-52).

9. As per claims 29 and 37, Drake and Porras disclose the system as recited in claims 1 and 36, wherein “enterprise latency mapping is performed” is taught by Drake in (Col 8 line 43 to Col 9 line 15).

10. As per claims 30 and 33, Drake and Porras disclose the system as recited in claims 29 and 32, However, Drake does not teach “at least one of the zone controllers chooses a port number associated with an application”. Nevertheless, Porras does include this feature in (Col 2 lines 12-17). Therefore, it would have been obvious at the time of the invention for one having ordinary skill in the art to modify Drake’s invention to implement port listening for a certain application to directly monitor the application for security breach.

11. As per claims 31 and 32, Drake and Porras disclose the system as recited in claims 30 and 31, wherein “the at least one zone controller pushes a configuration request to a plurality of the host controllers in an associated zone; and the host controllers push the configuration request to the agents” is taught by Drake in (Col 11

Art Unit: 2135

line 7 to Col 12 line 10, and Col 16 lines 53-57). The agent (Collector) sends the event info based on the expert system requests.

12. As per claim 34, Drake and Porras disclose the system as recited in claimed 33, wherein "monitor data is sent from the agents to the host controllers" is taught by Drake in (Col 10 lines 10-20, and Col 11 lines 5-25).

13. As per claim 35, Drake and Porras disclose the system as recited in claim 34, wherein "the monitor data is buffered" is taught by Drake in (Col 5 lines 20-30).

14. As per claim 36, Drake and Porras disclose the system as recited in claim 34, wherein "the host controllers update the at least one zone controller with consolidated monitor data" is taught by Drake in (Col 16 lines 53-67, and Figure 1, 16).

**15. Claims 2, 7, 12, 17, 23, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Drake in view of Porras, and further in view of Eschelbeck (U5/655337881).**

16. As per claims 2, 7, 12, and 17, Drake and Porras disclose the system as recited in claim 1. However, Drake and Porras do not teach the host controllers are further capable of cyber cop services. Nevertheless, Eschelbeck discloses the "System and process for reporting network events with a plurality of hierarchically-structured databases in a distributed computing environment" invention, which teaches a method

Art Unit: 2135

of analyzing, detecting, and response to a network node anomaly, such as intrusion, virus attack, and network attack (See Fig. 2). The system includes agents, event detectors and analyzer, and root snap-in agent. The event responding includes forwarding a snap-in component to control the anomaly (Col 7 lines 52-63 and Col 10 line 34 to Col 12 line 8). One of the snap-in components is the cyber cop service (Eschelbeck, Col 5 Line 34). Therefore, it is obvious at the time of the invention was made for one of ordinary skill in the art to incorporate the teaching to resolve the problem in the network.

17. As per claims 23 and 24, Claim 1 rejection is incorporated. However, Drake and Porras do not teach the anti-virus services. Nevertheless, Eschelbeck teaches the implementation of the anti-virus services (Col 7 lines 1-13). Therefore, it is obvious at the time of the invention for one of ordinary skill in the art to incorporate the service to check the data integrity in the network.

### ***Conclusion***

18. Applicant has amended claims 1,6,11,15,21,22,25, and 27, which necessitated new grounds of rejection. See Rejections above.

19. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP



***Response to Amendment***

18. Applicant has amended claims **1,6,11,15,21,22,25, and 27**, which necessitated new grounds of rejection. See Rejections above.

***Conclusion***

19. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).


20. A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

21. Any inquiry concerning this communication from the examiner should be directed to Linh Son whose telephone number is (571)-271-3856.

22. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor Kim Y. Vu can be reached at (571)-272-3859. The fax numbers for this group are (703)-872-9306 (official fax). Any inquiry of general nature or relating to the status of this application or proceeding should be directed to the group receptionist whose telephone number is (571)-272-2100.

23. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval IPAIR.I system. Status information for published applications may be obtained from either Private PMR or Public PMR. Status information for unpublished applications is available through Private PMR only. For more information about the PAIR system, see <http://pzd-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

**Linh LD Son**  
**Patent Examiner**

  
KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100